Further investigations on the QAM method for finding new APN functions

Nadiia Ichanska
(Joint work with Simon Berg and Nikolay S. Kaleyski)

University of Bergen

Selmer Seminar
March 18, 2024

Vectorial Boolean Functions and APN functions

F_{2^n} - finite field with 2^n elements, n 2 N.

- A function $F : F_{2^n} \; ! \; F_{2^n}$ is called **(n,n)-**function or **Vectorial Boolean Function**.

Vectorial Boolean Functions and APN functions

F_{2^n} - nite eld with 2^n elements,$n \in N$.

- A function $F : F_{2^n} \to F_{2^n}$ is called(n,n)- function or Vectorial Boolean Function.
- $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$; $a_i \in F_{2^n}$ - its univariate representation.

Vectorial Boolean Functions and APN functions

F_{2^n} - nite eld with 2^n elements,$n \in \mathbb{N}$.

- A function $F : F_{2^n} \to F_{2^n}$ is called(n,n)- function or Vectorial Boolean Function.
- $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$; $a_i \in F_{2^n}$ - its univariate representation.
- $D_a F(x) = F(a+x) + F(x)$ - its derivative in the direction $a \in F_{2^n} \setminus \{0\}$.

Vectorial Boolean Functions and APN functions

F_{2^n} - nite eld with 2^n elements,$n \ 2 \ N$.

- A function $F : F_{2^n} ! \ F_{2^n}$ is called(n,n)- function or Vectorial Boolean Function.
- $F(x) = \sum_{i=0}^{2^n \ 1} a_i \ x^i; \ a_i \ 2 \ F_{2^n}$ - its univariate representation.
- $D_a F(x) = F(a + x) + F(x)$ - its derivative in the direction $a \ 2 \ F_{2^n} nf \, 0g$.
- ${}_aF(x) = F(a + x) + F(x) + F(a) + F(0)$ - symmetric derivative in the direction$a \ 2 \ F_{2^n} nf \, 0g$ of F.

Vectorial Boolean Functions and APN functions

F_{2^n} - nite eld with 2^n elements,$n \in N$.

- A function $F : F_{2^n} \to F_{2^n}$ is called(n,n)- function or Vectorial Boolean Function.
- $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$; $a_i \in F_{2^n}$ - its univariate representation.
- $_aF(x) = F(a+x) + F(x) + F(a) + F(0)$ - symmetric derivative in the direction$a \in F_{2^n} \setminus \{0\}$ of F.

Vectorial Boolean Functions and APN functions

F_{2^n} - nite eld with 2^n elements,$n \in \mathbb{N}$.

- A function $F : F_{2^n} \to F_{2^n}$ is called(n,n)- function or Vectorial Boolean Function .
- $F(x) = \sum_{i=0}^{2^n-1} a_i x^i;\ a_i \in F_{2^n}$ - its univariate representation.
- $_aF(x) = F(a+x) + F(x) + F(a) + F(0)$ - symmetric derivative in the direction$a \in F_{2^n} \setminus \{0\}$ of F.
- $_F = \max_{a,b \in F_{2^n}, a \neq 0} |\{x \in F_{2^n} : {}_F(a,x) = b\}|$ - its di erential unifomity .

Vectorial Boolean Functions and APN functions

F_{2^n} - nite eld with 2^n elements,$n \in \mathbb{N}$.

- A function $F : F_{2^n} \to F_{2^n}$ is called(n,n)- function or Vectorial Boolean Function .
- $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$; $a_i \in F_{2^n}$ - its univariate representation.
- ${}_aF(x) = F(a+x) + F(x) + F(a) + F(0)$ - symmetric derivative in the direction$a \in F_{2^n} \setminus \{0\}$ of F.
- $_F = \max_{a,b \in F_{2^n}, a \neq 0} |\{x \in F_{2^n} : {}_F(a,x) = b\}|$ - its di erential unifomity .
- F is almost perfect nonlinear(APN) if $_F = 2$.

- The algebraic degree of a function $F : F_{2^n} \to F_{2^n}$ is $\deg(F) = \max_{0 \le i \le 2^n - 1, a_i \neq 0} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.

- The algebraic degree of a function $F : F_{2^n} \to F_{2^n}$ is $\deg(F) = \max_{0 \le i \le 2^n - 1, a_i \ne 0} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a linear function if $F(x) = \sum_{0 \le i < n} a_i x^{2^i}$; $a_i \in F_{2^n}$:

  F is a ne if it is a sum of a linear and a constant.

- The algebraic degree of a function $F : F_{2^n} \to F_{2^n}$ is $\deg(F) = \max_{0 \le i \le 2^n - 1, a_i \neq 0} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a linear function if $F(x) = \sum_{0 \le i < n} a_i x^{2^i}$; $a_i \in F_{2^n}$:
  F is a ne if it is a sum of a linear and a constant.
- F is quadratic if $\deg(F) = 2$.

- The algebraic degree of a function $F : F_{2^n} \to F_{2^n}$ is $\deg(F) = \max_{0 \le i \le 2^n - 1, a_i \neq 0} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a linear function if $F(x) = \sum_{0 \le i < n} a_i x^{2^i}$; $a_i \in F_{2^n}$:
  F is a ne if it is a sum of a linear and a constant.
- F is quadratic if $\deg(F) \le 2$.
- We will consider homogeneous quadratic (n, n)-function F

$$F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}; \quad a_{i,j} \in F_{2^n}:$$

Equivalence

The functions F and F^0 from F_{2^n} to itself are called

- a ne equivalent (or linear equivalent) if $F^0 = A_1 \quad F \quad A_2$ for a ne (linear) permutations $A_1; A_2$ from F_{2^n} to itself.

Equivalence

The functions F and F^0 from F_{2^n} to itself are called

- a ne equivalent (or linear equivalent) if $F^0 = A_1 \quad F \quad A_2$ for a ne (linear) permutations $A_1; A_2$ from F_{2^n} to itself.
- EA-equivalent if F^0 and $F + A$ are a ne equivalent for a ne mapping A.

Equivalence

The functions F and F^0 from F_{2^n} to itself are called

- a ne equivalent (or linear equivalent) if $F^0 = A_1 \quad F \quad A_2$ for a ne (linear) permutations $A_1; A_2$ from F_{2^n} to itself.
- EA-equivalent if F^0 and $F + A$ are a ne equivalent for a ne mapping A.
- Carlet-Charpin-Zinoviev(CCZ-equivalent).

Equivalence

The functions F and F^0 from F_{2^n} to itself are called

- a ne equivalent (or linear equivalent) if $F^0 = A_1 \quad F \quad A_2$ for a ne (linear) permutations $A_1; A_2$ from F_{2^n} to itself.
- EA-equivalent if F^0 and $F + A$ are a ne equivalent for a ne mapping A.
- Carlet-Charpin-Zinoviev(CCZ-equivalent).
  For quadratic APN $(n; n)$ - functions, F and F^0 are CCZ-equivalent if and only if they are EA-equivalent [2].

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over $\mathbb{F}_{2^n}$.

QAM of the quadratic function over F_{2^n}

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over F_{2^n}.
- Let us set a normal basis $B = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of F_{2^n} over F_2.

QAM of the quadratic function over F_{2^n}

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over F_{2^n}.
- Let us set a normal basis $B = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of F_{2^n} over F_2.
- [3] The rank of the vector $v \in F_{2^n}^n$ is the dimension of the subspace spanned by its elements.

QAM of the quadratic function over F_{2^n}

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over F_{2^n}.
- Let us set a normal basis $B = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of F_{2^n} over F_2.
- [3] The rank of the vector $v \in F_{2^n}^n$ is the dimension of the subspace spanned by its elements.
- The derivative matrix $M_F \in F_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} \partial_b F(b) & \partial_b F(b^2) & \ldots & \partial_b F(b^n) \\ \partial_{b^2} F(b) & \partial_{b^2} F(b^2) & \ldots & \partial_{b^2} F(b^n) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{b^n} F(b) & \partial_{b^n} F(b^2) & \ldots & \partial_{b^n} F(b^n) \end{bmatrix}.$$

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The derivative matrix M_F 2 $F_{2^n}^{n\ n}$ of function F is

$$M_F = \begin{matrix} 2 \\ 6 \\ 6 \\ 4 \end{matrix} \begin{matrix} F(b;b) & F(b;b^2) & \vdots\vdots & F(b;b^n) \\ F(b;b^2) & F(b^2;b^2) & \vdots\vdots & F\ b^2;b^n \\ \vdots & \vdots & \ddots & \vdots \\ F(b;b^n) & F\ b^2;b^n & \vdots\vdots & F(b^n;b^n) \end{matrix} \begin{matrix} 3 \\ 7 \\ 7 \\ 5 \end{matrix} : \quad (1)$$

QAM of the quadratic function over F_{2^n}

- The derivative matrix $M_F \in F_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} F(b;b) & F(b;b^2) & \cdots & F(b;b^n) \\ F(b;b^2) & F(b^2;b^2) & \cdots & F(b^2;b^n) \\ \vdots & \vdots & \ddots & \vdots \\ F(b;b^n) & F(b^2;b^n) & \cdots & F(b^n;b^n) \end{bmatrix}. \quad (1)$$

- A matrix $M_F \in F_{2^n}^{n \times n}$ is called a Quadratic APN Matrix (QAM) [3] if:

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The derivative matrix $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} 2 & & & & 3 \\ F(b;b) & F(b;b^2) & \cdots & F(b;b^n) \\ 6 & 7 \\ F(b;b^2) & F(b^2;b^2) & \cdots & F\left(b^2;b^n\right) \\ 6 & 7 \\ 6 & 7 \\ 4 & \vdots & \vdots & \ddots & \vdots \\ F(b;b^n) & F\left(b^2;b^n\right) & \cdots & F(b^n;b^n) & 5 \end{bmatrix}. \quad (1)$$

- A matrix $M_F \in \mathbb{F}_{2^n}^{n \times n}$ is called a Quadratic APN Matrix (QAM) [3] if:
  1. M_F is symmetric and the elements in its main diagonal are all zeros;

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The derivative matrix $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} 0 & F(b;b) & F(b;b^2) & \cdots & F(b;b^n) \\ F(b;b^2) & 0 & F(b^2;b^2) & \cdots & F(b^2;b^n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F(b;b^n) & F(b^2;b^n) & \cdots & F(b^n;b^n) & 0 \end{bmatrix}. \quad (1)$$

- A matrix $M_F \in \mathbb{F}_{2^n}^{n \times n}$ is called a Quadratic APN Matrix (QAM) [3] if:
  1. M_F is symmetric and the elements in its main diagonal are all zeros;
  2. Every nonzero linear combination of the n rows (or columns, since M_F is symmetric) of M_F has rank $n-1$.

Following Corollary 5 from [1], we get that function

$$F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}, \; a_{i,j} \in F_{2^n} \qquad (2)$$

is APN if and only if its derivative matrix M_F is QAM.

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in F_{2^m}$ in some subfield F_{2^m} of F_{2^n}

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in F_{2^m}$ in some subfield F_{2^m} of F_{2^n}
- $(F(x))^{2^m} = \left(a_i^{2^m}\right) \left(x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m} = F\left(x^{2^m}\right)$,

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \le i<j \le n-1} a_{i,j} x^{2^i+2^j}$ with coefficients $a_{i,j} \in F_{2^m}$ in some subfield F_{2^m} of F_{2^n}
- $(F(x))^{2^m} = \left(a_i^{2^m} \left(x^i\right)^{2^m}\right) = \left(\sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m}\right) = F\left(x^{2^m}\right)$,
- $\left({}_aF(x)\right)^{2^m} = F(x+a)^{2^m} + F(x)^{2^m} + F(a)^{2^m} = {}_{a^{2^m}}F\left(x^{2^m}\right)$,

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in F_{2^m}$ in some subfield F_{2^m} of F_{2^n}
- $(F(x))^{2^m} = \left(a_i^{2^m}\right) \left(x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m} = F\left(x^{2^m}\right)$,
- $\left({}_aF(x)\right)^{2^m} = F(x+a)^{2^m} + F(x)^{2^m} + F(a)^{2^m} = {}_{a^{2^m}}F\left(x^{2^m}\right)$,

$$M_{i+m;j+m} = \left(M_{i,j}\right)^{2^m}:$$

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \le i<j \le n-1} a_{i,j} x^{2^i+2^j}$ with coefficients $a_{i,j} \in F_{2^m}$ in some subfield F_{2^m} of F_{2^n}
- $(F(x))^{2^m} = \left(\sum_i a_i x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i x^{i\,2^m} = F\left(x^{2^m}\right)$,
- $\left({}_aF(x)\right)^{2^m} = F(x+a)^{2^m} + F(x)^{2^m} + F(a)^{2^m} = {}_{a^{2^m}}F\left(x^{2^m}\right)$,

$$M_{i+m;j+m} = (M_{i;j})^{2^m}:$$

$$\begin{pmatrix} 0 & F(b_1;b_2) & \cdots & \cdots & F(b_1;b_n) \\ F(b_1;b_2) & 0 & \ddots & \cdots & F(b_2;b_n) \\ \vdots & \ddots & \ddots & (F(b_1;b_2))^{2^m} & \vdots \\ \vdots & \ddots & (F(b_1;b_2))^{2^m} & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ F(b_1;b_n) & F(b_2;b_n) & \cdots & \cdots & 0 \end{pmatrix}$$

Structure of the search

$$M_F = \begin{pmatrix} 0 & 0 & 1 & 2 & \cdots & \cdots & \cdots & 1 \\ 1 & 0 & \ddots & \ddots & \cdots & \cdots & & \\ 2 & \vdots & 0 & 2^m_1 & 2^m_2 & \cdots & & \\ \vdots & \vdots & 2^m_1 & 0 & \cdots & \cdots & & \\ \vdots & \vdots & 2^m_2 & \cdots & 0 & \cdots & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & \end{pmatrix}; \qquad (3)$$

where $_1; \ _2; : : : ; \ _l \ 2 \ F_{2^n}$ - variables.

Structure of the search

$$M_F = \begin{pmatrix} 0 & 0 & 1 & 2 & \cdots & \cdots & \cdots & 1 \\ 1 & 0 & \ddots & \ddots & \cdots & \cdots & & \\ 2 & \vdots & 0 & 2^m_1 & 2^m_2 & \cdots & & \\ \vdots & \vdots & 2^m_1 & 0 & \cdots & \cdots & & \\ \vdots & \vdots & 2^m_2 & \cdots & 0 & \cdots & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & \end{pmatrix}; \qquad (3)$$

where $_1$; $_2$; : : : ; $_l$ 2 F_{2^n} - variables.
A variable $_i$ is located on the i-th level.

Orbit restrictions

Theorem 3 [3]

For any linear permutation l on F_{2^n} and $M \in F_{2^n}^{n \times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i, j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent(also EA-equivalent) to F.

Orbit restrictions

Theorem 3 [3]

For any linear permutation l on F_{2^n} and $M \in F_{2^n}^{n \times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i, j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent(also EA-equivalent) to F.

Let L be a set of all linear (n, n)-permutations $l = \sum_{i=1}^{n} \alpha_i x^{2^i - 1}$ on F_{2^n} with sub eld $\alpha_i \in F_{2^m}$.

Orbit restrictions

Theorem 3 [3]

For any linear permutation l on F_{2^n} and $M \in F_{2^n}^{n \times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i, j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent(also EA-equivalent) to F.

Let L be a set of all linear (n, n)-permutations $l = \sum_{i=1}^{n} \alpha_i x^{2^i - 1}$ on F_{2^n} with sub field $\alpha_i \in F_{2^m}$. Then the orbit of $a \in F_{2^n}$

$$Orb(a, L) = \{l(a) : l \in L\}. \tag{5}$$

Orbit Restrictions

$$F_{2^n} = \mathrm{Orb}(a_1; L) \cup \cdots \cup \mathrm{Orb}(a_k; L), \text{ for some } a_i \in F_{2^n},\ 1 \le i \le k.$$

Orbit Restrictions

$$F_{2^n} = \mathrm{Orb}(a_1; L) \cup \cdots \cup \mathrm{Orb}(a_k; L); \text{ for some } a_i \in F_{2^n};\ 1 \le i \le k.$$

$$M_{F^0} = \begin{pmatrix} 0 & 0 & L(\alpha_1) & L(\alpha_2) & \cdots & \cdots & \cdots & 1 \\ L(\alpha_1) & 0 & \ddots & \ddots & \cdots & \cdots & \cdots & \\ L(\alpha_2) & \vdots & 0 & L(\alpha_1^{2^m}) & L(\alpha_2^{2^m}) & \cdots & \cdots & \\ \vdots & \vdots & L(\alpha_1^{2^m}) & 0 & \cdots & \cdots & \cdots & \\ \vdots & \vdots & L(\alpha_2^{2^m}) & \cdots & 0 & \cdots & \cdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & \end{pmatrix};$$

where $L(\alpha_i^{2^{m-j}}) = (L(\alpha_i))^{2^{m-j}}$; $j \in \{1, \ldots, n/m - 1\}$ for any variable α_i; $1 \le i \le l$.

Orbit partition level by level

$$F_{2^n} = \mathrm{Orb}(A; L) [\ : : : ; \ A \ 2 \ F_{2^n} :$$

Orbit partition level by level

$$F_{2^n} = \mathrm{Orb}(A; L)[\ \vdots\ ;\ A^2\ F_{2^n}\ \vdots$$

$$M_F = \begin{pmatrix} 0 & 0 & A & \cdots & \cdots & 1 \\ 0 & 0 & \ddots & \ddots & \cdots & \cdots \\ A & \cdots & 0 & A^{2^m} & \cdots & \cdots \\ A^2 & \vdots & A^{2^m} & 0 & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \cdots \\ 1 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

Orbit partition level by level

$$F_{2^n} = \mathrm{Orb}(A; L) \left[\ldots; A^2 F_{2^n} \right.:$$

$$M_F = \begin{pmatrix} 0 & 0 & A & \cdots & \cdots & \cdots & 1 \\ 0 & A & 0 & \ddots & \ddots & \cdots & \cdots \\ A & 0 & \ddots & 0 & A^{2^m} & A^{2^m} & \cdots \\ A^2 & \cdots & 0 & A^{2^m} & 0 & \cdots & \cdots \\ \vdots & \vdots & A^{2^m} & 0 & \cdots & 0 & \cdots \\ \vdots & \vdots & A^{2^m} & \cdots & 0 & \cdots & A \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \end{pmatrix}:$$

$$\mathrm{Orb}_A(A^2; L) = \{ l(A^2) : l \in L \mid l(A) = A \}.$$

Orbit partition level by level

$$F_{2^n} = \mathrm{Orb}(A; L) \left[\; : : : ; \; A^{2} \; F_{2^n} : \right.$$

$$M_F = \begin{pmatrix} 0 & A & \cdots & \cdots & \cdots & 1 \\ A & 0 & \ddots & \ddots & \cdots & \cdots \\ \vdots & \vdots & 0 & A^{2^m} & \cdots & \cdots \\ \vdots & \vdots & A^{2^m} & 0 & \cdots & \cdots \\ \vdots & \vdots & \cdots & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} :$$

$$\mathrm{Orb}_A(\; ; L) = \{ l(\;) : l \in L \mid l(A) = A \}.$$

$$S = \{ \; ; : : : ; \; \}$$

$$\mathrm{Orb}_S(\; ; L) = \{ l(\;) : l \in L \mid \forall X \in S : \; l(X) = X \}.$$

Submatrix method

- Let $M \in F_{2^n}^{n \times n}$ be a derivative matrix.

Submatrix method

- Let $M \in F_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in F_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is proper.

Submatrix method

- Let $M \in F_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in F_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is proper.
- S proper if every nonzero linear combinations of the p rows has rank at least $q - 1$.

Submatrix method

- Let $M \in F_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in F_{2^n}^{p \times q}$, $1 \le p, q \le n$ of M is proper.
- $$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & A & B & A^3 & \cdots & \\ A & 0 & \ddots & \ddots & \cdots & \\ B & \vdots & 0 & A^{2^m} & B^{2^m} & \cdots \\ A^3 & \vdots & A^{2^m} & 0 & \cdots & \\ \vdots & \vdots & B^{2^m} & \cdots & 0 & \cdots \end{pmatrix}$$

Submatrix method

- Let $M \in F_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in F_{2^n}^{p \times q}$, $1 \le p, q \le n$ of M is proper.
- $$\begin{pmatrix} 0 & 0 & A & B & A^3 & \cdots & \cdots & 1 \\ 0 & A & B & A^3 & \ddots & \cdots & \cdots & \\ A & B & A^3 & \ddots & \ddots & \cdots & \cdots & \\ B & A^3 & \ddots & \ddots & A^{2^m} & B^{2^m} & \cdots & \\ A^3 & \vdots & \ddots & A^{2^m} & B^{2^m} & \cdots & \cdots & \\ \vdots & \vdots & A^{2^m} & B^{2^m} & \cdots & \cdots & \cdots & \end{pmatrix}$$
- After considering $F^0 = F \setminus L$, where $L = \{a_j x^{2^i} : a_j \in F_{2^m}\}$, we could eliminate the number of submatrices for this test.

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.
- $4^8 = 65536$ linear permutations with coe cients in the sub eld were constructed.

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.
- $4^8 = 65536$ linear permutations with coe cients in the sub eld were constructed.
- By using these permutations, the rst level of the search was partitioned into 4 orbits.

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.
- $4^8 = 65536$ linear permutations with coe cients in the sub eld were constructed.
- By using these permutations, the rst level of the search was partitioned into 4 orbits.

1	a	a^7	a^{17}

Table: The rst level

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.
- $4^8 = 65536$ linear permutations with coe cients in the sub eld were constructed.
- The number of variables = levels in this dimension is 8.
- By using these permutations, the rst level of the search was partitioned into 4 orbit representatives.

1	a	a^7	a^{17}
$\#\, f\ {}_2g_i = 8$ $Orb_{1\ 2}$	$\#\, f\ {}_2g_i = 30$ $Orb_{a\ 2}$	$\#\, f\ {}_2g_i = 22$ $Orb_{a^7\ 2}$	$\#\, f\ {}_2g_i = 14$ $Orb_{a^{17}\ 2}$

Table: The second level

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

- 196863 quadratic APN functions were found in the search, with 27 unique ortho-derivative di erential spectra.

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

- 196863 quadratic APN functions were found in the search, with 27 unique ortho-derivative di erential spectra.
- $a^{85}x^{96} + a^{85}x^{72} + a^{170}x^{24} + x^{18} + a^{85}x^{12} + a^{85}x^9 + x^6 + x^3$.

(8,2)

- $F(x)$ over F_{2^8} with coe cients in F_{2^2}.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

- 196863 quadratic APN functions were found in the search, with 27 unique ortho-derivative di erential spectra.
- $a^{85}x^{96} + a^{85}x^{72} + a^{170}x^{24} + x^{18} + a^{85}x^{12} + a^{85}x^9 + x^6 + x^3$.
- $0^{38196}; 2^{22008}; 4^{4608}; 6^{456}; 8^{12}$ - its ortho-derivative di erential spectra.

(10,2)

- $F(x)$ over $F_{2^{10}}$ with coe cients in F_{2^2}.
- $4^{10} = 1048576$ linear permutations with coe cients in the sub eld were constructed.
- The number of variables = levels in this dimension is 9.
- By using these permutations, the rst level of the search was partitioned into 3 orbit representatives.

1	a	a^5
# f $_2$g$_i$ = 5 Orb$_1$ $_2$	# f $_2$g$_i$ = 33 Orb$_a$ $_2$	# f $_2$g$_i$ = 50 Orb$_{a^5}$ $_2$

(10,1)

- $F(x)$ over $F_{2^{10}}$ with coe cients in F_{2^1}.
- $2^{10} = 1024$ linear permutations with coe cients in the sub eld were constructed.
- The number of variables = levels in this dimension is 5.
- By using these permutations, the rst level of the search was partitioned into 8 orbit representatives.

1	a	a^5	a^{15}	a^{33}	a^{57}	a^{99}	a^{341}
# of orbit representatives for 2^{nd} level after Sub-matrix Test							
0	746	1012	753	71	112	78	8

(9,3)

- $F(x)$ over F_{2^9} with coe cients in F_{2^3}.
- $8^9 = 134217728$ linear permutations with coe cients in the sub eld were constructed.
- The number of variables = levels in this dimension is 12.

(9,3)

- $F(x)$ over F_{2^9} with coe cients in F_{2^3}.
- $8^9 = 134217728$ linear permutations with coe cients in the sub eld were constructed.
- The number of variables = levels in this dimension is 12.

Remark

Let $a \in F_{2^9}$. We categorize a into the following cases:

1. $Cat_1 = \{a : a \in F_{2^9} \mid a + a^{2^3} = 0\}$,
2. $Cat_2 = \{a : a \in F_{2^9} \mid a + a^{2^3} + a^{2^6} = 0\}$,
3. $Cat_3 = \{a : a \in F_{2^9} \mid a \neq Cat_1;\ a \neq Cat_2\}$,

(9,3)

- $F(x)$ over F_{2^9} with coefficients in F_{2^3}.
- $8^9 = 134217728$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 12.

Remark

Let $a \in F_{2^9}$. We categorize a into the following cases:

1. $Cat_1 = \{a : a \in F_{2^9} \mid a + a^{2^3} = 0\}$,
2. $Cat_2 = \{a : a \in F_{2^9} \mid a + a^{2^3} + a^{2^6} = 0\}$,
3. $Cat_3 = \{a : a \in F_{2^9} \mid a \notin Cat_1;\ a \notin Cat_2\}$,

Theorem

Let $a, b \in Cat_3$. If there exist $l(x) = \sum_{i=0}^{8} c_i x^{2^i};\ c_i \in F_{2^3}$ s.t. $l(a) = b;\ l(a^{2^3}) = b^{2^3};\ l(a^{2^6}) = b^{2^6}$. Then there exist linear permutation $L \in \mathcal{L}$ s.t. $L(a) = b$.

Conclusions

- For $F(x)$ over F_{2^n} with coe cients in F_{2^m} we run searches $(n; m)$ for $(8; 2); (10; 2); (10; 1); (9; 3)$.

Conclusions

- For $F(x)$ over F_{2^n} with coe cients in F_{2^m} we run searches $(n; m)$ for $(8; 2); (10; 2); (10; 1); (9; 3)$.
- We conclude where it is feasible to get the results and improve the computational method as possible.

Conclusions

- For $F(x)$ over F_{2^n} with coefficients in F_{2^m} we run searches $(n; m)$ for $(8; 2); (10; 2); (10; 1); (9; 3)$.
- We conclude where it is feasible to get the results and improve the computational method as possible.
- Computational searches are still running.


Diana Davidova and Nikolay Kaleyski.
Classification of all do planar polynomials with prime field coefficients over $gf(3^n)$ for n up to 7.
Cryptology ePrint Archive, Paper 2022/1059, 2022.
https://eprint.iacr.org/2022/1059.


Satoshi Yoshiara.
Equivalences of quadratic APN functions.
Journal of Algebraic Combinatorics, 35(3):461–475, 2012.


Yuyin Yu, Mingsheng Wang, and Yongqiang Li.
A matrix approach for constructing quadratic APN functions.
Designs, codes and cryptography, 73(2):587–600, 2014.